

# I business partner di Akhela per la sicurezza logica

---

## Soluzioni per la fase di valutazione

### View Suite - Skybox Security

---

View Suite è la prima suite integrata di applicazioni per la gestione dei rischi informatici che, partendo dalla valutazione delle vulnerabilità e dall'analisi dei rischi, arriva alla definizione del piano di azione per la gestione di eventi che possono mettere a rischio il sistema informativo di un'azienda. Si tratta di un'applicazione non intrusiva, in grado di distinguere, tra tutte le vulnerabilità, quelle che incidono gravemente sulle applicazioni critiche di business, sia che l'origine dell'attacco arrivi dall'interno della società, sia che arrivi dall'esterno.

### AVDS - Beyond Security

---

AVDS (Automated Vulnerability Detection System) realizza una mappatura della rete dell'organizzazione simulando attacchi originati sia dall'interno che dall'esterno e testando le vulnerabilità a livello network (switch, router, firewall porte etc.), sistema (Microsoft, Unix, Linux, Bsd etc.) applicazione (web server, database, mail server applicazioni ecc.). Completata la mappatura, viene generato un rapporto dettagliato nel quale sono elencati i tipi di attacco realizzati e le vulnerabilità trovate, a fronte delle quali vengono presentate diverse soluzioni. Viene inoltre predisposto un rapporto di facile lettura che permette ai responsabili dell'organizzazione di avere una visione dettagliata dei problemi di sicurezza della propria rete. Tali attività possono essere eseguite con scadenze predefinite. AVDS viene aggiornato giornalmente alla ricerca delle più recenti vulnerabilità, mantenendo in tal modo costantemente protetta l'infrastruttura del cliente.

## Soluzioni per la fase di implementazione

### Breachgate Sitegrity - Breach

---

Sitegrity è stato implementato per impedire che informazioni o transazioni corrotte vengano pubblicate in un sito web. E' basato sulla tecnologia ExitControl ed effettua in tempo reale una analisi dettagliata di ogni oggetto che viene inviato dal web server, assicurando che tutto il contenuto, sia esso statico o dinamico, come pure tutte le web applications siano autentiche ed inalterate. Ogni dato che potrebbe essere stato modificato viene rimpiazzato con del contenuto originale ed autentico. Di conseguenza, anche se un hacker dovesse riuscire ad entrare nel sito, i contenuti dello stesso all'esterno rimarrebbero intatti.

### Network Vault - Cyber-Ark

---

Cyber-Ark rivoluziona l'approccio nei confronti della sicurezza informatica partendo dal concetto della cassaforte: integra infatti strettamente diverse tecnologie di sicurezza per costruire il luogo più sicuro possibile per le infrastrutture di rete, indipendentemente dalla sicurezza della rete a livello generale. I dati nel Network Vault non sono mai manipolati o trattati, assicurando in tal modo che essi stessi non possano rappresentare un pericolo per la sicurezza del sistema. La metodologia di isolamento dei dati crea un ambiente sterile sulla base del quale possono essere costruiti ulteriori livelli di sicurezza. L'accesso alla cassaforte virtuale è protetto da sistemi basati sull'autenticazione forte degli utenti, con accessi limitati a determinati ambienti, sessioni cifrate di ingresso, e tutti i dati inseriti sono ispezionati in modo dettagliato. Network Vault risiede su un computer dedicato sul quale è l'unico software installato. Lo specifico firewall permette solo al protocollo dedicato di fare uscire ed entrare dati in questo computer.

# I business partner di Akhela per la sicurezza delle infrastrutture

---

## Endpoint Access Manager – Control Guard

---

Endpoint Access Manager è la prima piattaforma che affronta il problema della sicurezza dei dati nel momento del loro utilizzo quotidiano. E' basato su un agente software installato su portatili, desktop e server che controlla e registra continuamente l'utilizzo dei dati da parte dei soggetti facenti parte dell'organizzazione. Tutte le attività relative all'accesso ed al movimento delle informazioni sono controllate e registrate, e possono essere bloccate o semplicemente segnalate con degli alert all'amministratore del sistema e/o all'end-user.

## Intellinx

---

Intellinx è un software innovativo che permette di monitorare il comportamento degli utilizzatori finali nei sistemi legacy ed in altre piattaforme in ambiente mainframe e web. Intellinx introduce infatti una nuova dimensione nelle ispezioni e nell'analisi delle frodi: la capacità di registrare l'interazione di tutti gli utenti finali con le applicazioni centrali, permettendo di zoomare sull'attività di utilizzatori sospetti. Intellinx è indirizzato a tutte le grandi aziende che devono rispettare i requisiti di Basilea 2 e che, in generale, sono tenute a tenere traccia di qualsiasi operazione che venga fatta sui dati, anche al fine di garantire la privacy.

## Soluzioni per la fase di gestione

## Operations Manager – Blade Logic

---

Una soluzione software Enterprise-Class che automatizza il ciclo di vita completo della gestione dei server, consentendo di configurare un numero n di server secondo un modello predefinito o di verificarne la compliance rispetto a questo.

## Commtouch – Antispam Enterprise Solution

---

Anti-Spam Enterprise Solution Commtouch è la piattaforma antispam più affidabile (97% di successo sul controllo in rapporto ai più bassi livelli di falsi positivi registrati). E' configurabile e gestibile in maniera centralizzata per l'intera rete aziendale.

## Spy Sweeper – Webroot Software

---

La soluzione per anti-spyware, blocco popup, accesso a dati personali ed altri rischi insiti nell'utilizzo di e-mail e navigazione web, configurabile e gestibile in maniera centralizzata per l'intera rete aziendale. Spy Sweeper è l'unico programma a possedere una tecnologia a scudi attivi che blocca gli spyware prima che possano infettare il computer. Scansioni profonde estirpano e mettono in quarantena i programmi più ingannevoli.

## Breachview SSL – Breach

---

BreachView SSL è un modulo che ha lo scopo di controllare il traffico che avviene via SSL e che è in grado di risolvere il grande problema legato a tale protocollo, quello degli attacchi che possono essere portati contro l'intrusion detection system. Infatti, i sensori IDS non sono in grado di decifrare l'SSL. Di conseguenza, il traffico criptato su SSL viaggia senza essere esaminato. BreachView SSL gestisce il traffico via SSL fornendo testo comprensibile al sensore IDS, senza terminare la sessione. Viene così aumentata enormemente la visibilità dell'IDS sul traffico più critico della rete.

akhela

Sesta Strada Ovest - Z.I. Macchiareddu  
I-09010 Uta (CA)  
Tel. 070/24661000  
Fax 070/24661111

Via Larga, 13  
I-20122 Milano  
Tel. 02/7737472  
Fax 02/7737449

Viale dell'Esperanto, 71  
I-00144 Roma  
Tel. 06/54210205  
Fax 06/5912826

www.akhela.com  
info@akhela.com